UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/001,410	10/31/2001	George S. Gales	10017028-1	3057

7590 07/20/2006

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
SHERKAT, AREZOO	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 07/20/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/001,410	GALES ET AL.	
	Examiner	Art Unit	
	Arezoo Sherkat	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 April 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 October 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Reopening of Prosecution - New Ground of Rejection After Appeal Brief

In view of the Appeal Brief filed on 4/20/2006, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 20-25 and 27are rejected under 35 U.S.C. 102(e) as being anticipated by Farley et al., (U.S. Publication No. 2002/0078381 and Farley hereinafter).

Regarding claim 20, Farley discloses a system of defining security vulnerabilities of a computer system, comprising:

generating a human-readable and a machine-readable vulnerability description language (VDL) file (i.e., the event log file 610 can comprise, human and machine-readable files, having comma separated values that store computer event data from an intrusion detection system – page 8, par. 0094) containing a definition of at least one vulnerability, and a definition of at least one policy item for detecting the vulnerability (i.e. the set of correlation events and corresponding correlation rules)(page 11, par 0126-0145);

an interpreter (i.e., event reader 600) operable to parse the at least one vulnerability definition and at least one policy item definition in the VDL file and organize the parsed definitions pursuant to a predetermined format (i.e., the event reader 600 reads in comma separated values in the event log file 610 and creates data objects that are processed by other software components on a fusion engine 22)(page 8, par. 0093-0094); and

a data storage operable to store the parsed and organized at least one vulnerability and at least one policy item definition (i.e., event classification database 635), wherein the data storage is accessible by at least one vulnerability scanner

application (i.e. computer events reported from detectors of intrusion detection systems)(page 8, par. 0098 and page 9, par. 0109).

Regarding claim 21, Farley discloses wherein the data storage is a relational database having a plurality of tables (page 8, par. 0098).

Regarding claim 22, Farley discloses wherein the VDL file further comprises a definition of a vulnerability scanner application (i.e., a host or a network detector, a firewall, or an audit system scan raw network traffic or local system events for predefined patterns)(page 5, par. 0065-0066 and page 8, par. 0097).

Regarding claim 23, Farley discloses wherein the VDL file further comprises a definition of a security category (i.e., the type parameter of a given raw event) providing a grouping of the at least one vulnerability, and a definition of a policy group providing a grouping of the at least one policy item (i.e., the type parameter of a given raw event corresponds to a number of rules)(page 11, par 0123-0126).

Regarding claim 24, Farley discloses wherein the VDL file further comprises a definition of at least one attribute of the at least one vulnerability (i.e., the CoBRA processor determines the risk of a raw computer event by assessing the event type parameter 555 in combination with environmental factors such as the destination

Internet protocol address of an attack in addition to the source of the attack)(page 8, par. 0096).

Regarding claim 25, Farley discloses wherein the VDL file further comprises an identification of the severity of risk associated with the at least one vulnerability attack (i.e., the raw event classification database 635 can categorize raw events based on their impact on the target host such as confidentiality, integrity, or availability)(page 8, par. 0098-0099).

Regarding claim 27, Farley discloses wherein the VDL file further comprises a definition of an application operable to respond to detecting the at least one vulnerability (i.e., a host or a network detector, a firewall, or an audit system)(page 5, par. 0065-0066).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-19 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Farley et al., (U.S. Publication No. 2002/0078381 and Farley hereinafter), in view of Chefalas et al., (U.S. Publication No. 2002/0116639 and Chefalas hereinafter).

Regarding claim 1, Farley discloses a method of defining the security vulnerability of a computer system, comprising:

generating a human-readable and a machine-readable vulnerability description language (VDL) file (i.e., event log file 610) specifying: an attack representing a recognized vulnerability of the computer system (i.e., each raw event received by the event reader 600 has been assigned a type or categorization based upon the intrusion detection system that generated the raw event)(page 8, par. 0094), at least one attribute (i.e., event type parameter 555) of the specified attack (i.e., the CoBRA processor determines the risk of a raw computer event by assessing the event type parameter 555 in combination with environmental factors)(page 8, par. 0096), and at least one policy definition with respect to detecting the vulnerability of the specified attack (i.e. the set of correlation events and corresponding correlation rules)(page 11, par 0126-0145).

Farley does not expressly disclose specifying a remedy for the specified vulnerability.

However, Chefalas discloses specifying a remedy for the specified vulnerability (i.e., action to be taken to mitigate the attack)(page 4, par. 0047-0048).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Farley with teachings of

Chefelas because it would allow to include specifying a remedy for the specified vulnerability as disclosed by Chefalas. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Chefalas to have an improved method and apparatus for providing a service for the detection, notification and elimination of computer viruses (Chefalas, page 1, par. 0011).

Regarding claims 12 and 2, Farley discloses a method of defining the security vulnerability condition of a system, comprising:

generating a human-readable and a machine-readable vulnerability description language (VDL) file (i.e., event log file 610) specifying: a name of a vulnerability associated with the system (i.e., each raw event received by the event reader 600 has been assigned a type or categorization based upon the intrusion detection system that generated the raw event)(page 8, par. 0094), at least one attribute (i.e., event type parameter 555) of the specified vulnerability (i.e., the CoBRA processor determines the risk of a raw computer event by assessing the event type parameter 555 in combination with environmental factors)(page 8, par. 0096), a policy definition with respect to detecting the vulnerability of the specified vulnerability (i.e., correlation rules corresponding to the set of correlation events), and at least one attribute of the specified policy definitions (i.e., the set of correlation events)(page 11, par 0126-0145).

Farley does not expressly disclose specifying a remedy for the specified vulnerability.

However, Chefalas discloses specifying a remedy for the specified vulnerability (i.e., action to be taken to mitigate the attack)(page 4, par. 0047-0048).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Farley with teachings of Chefelas because it would allow to include specifying a remedy for the specified vulnerability as disclosed by Chefalas. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Chefalas to have an improved method and apparatus for providing a service for the detection, notification and elimination of computer viruses (Chefalas, page 1, par. 0011).

Regarding claims 3 and 13, Farley discloses further comprising generating the VDL file specifying a computing platform of the computer system (i.e., the function of a data source 28 is to provide the event collector 24 with various types of information as it may relate to the network, host, or a single computer being monitored by the security management system 20)(page 5, par. 0063-0066).

Regarding claims 4 and 14, Farley discloses further comprising:

specifying a security category of the specified attack (i.e., the type parameter of a given raw event), and specifying at least one policy group with respect to the specified security category (i.e., the type parameter of a given raw event corresponds to a number of rules)(page 11, par 0123-0126).

Regarding claims 5 and 15, Farley discloses further comprising generating the VDL file specifying a vulnerability scanner executing on the computer system (i.e., a data source/detector 28 can comprise a host or a network detector, a firewall, or an audit system that scans raw network traffic or local system events for predefined patterns)(page 5, Par. 0065-0066 and page 8, par. 0097).

Regarding claims 6 and 16, Farley discloses specifying an identification of the severity associated with a breach of the computer system by the attack (i.e., the raw event classification database 635 can categorize raw events based on their impact on the target host such as confidentiality, integrity, or availability)(page 8, par. 0098-0099).

Regarding claim 7, Farley discloses wherein specifying at least one attribute of the specified attack comprises specifying a description of the attack (i.e., the CoBRA processor determines the risk of a raw computer event by assessing the event type parameter 555 in combination with environmental factors such as the destination Internet protocol address of an attack in addition to the source of the attack)(page 8, par. 0096).

Regarding claims 8 and 17, Farley discloses wherein specifying at least one attribute of the specified attack comprises specifying an explanation of why the specified attack is important (i.e., the raw event classification database 635 can categorize raw

events based on their impact on the target host such as confidentiality, integrity, or availability)(pages 8-9, par. 0098-0099).

Regarding claims 9 and 18, Farley does not disclose specifying at least one attribute of the specified attack comprises specifying how information is to be reported to a user with respect to the specified attack (i.e., as a mitigation action in response to detection of the specified attack).

However, Chefalas discloses specifying how information is to be reported to a user with respect to the specified attack (i.e., action to be taken to mitigate the attack)(page 4, par. 0047-0048).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Farley with teachings of Chefelas because it would allow to include how information is to be reported to a user with respect to the specified attack as disclosed by Chefalas. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Chefalas to have an improved method and apparatus for providing a service for the detection, notification and elimination of computer viruses (Chefalas, page 1, par. 0011).

Regarding claims 10, 19, and 26, Farley does not disclose specifying at least one attribute of the specified attack comprises specifying how information is to be reported

to a user with respect to the specified attack (i.e., as a mitigation action in response to detection of the specified attack).

However, Chefalas discloses wherein specifying at least one attribute of the specified attack comprises specifying a source of a remedy operable to fix the specified vulnerability (i.e., automatically paging a manager, a technician, or scheduling a service are some actions that may be offered)(page 4, par.0048-0051).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Farley with teachings of Chefelas because it would allow to include specifying a source of a remedy operable to fix the specified vulnerability as disclosed by Chefalas. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Chefalas to have an improved method and apparatus for providing a service for the detection, notification and elimination of computer viruses (Chefalas, page 1, par. 0011).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Barton et al., (U.S. Patent No. 6,944,775).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

A.S.

Patent Examiner
Group 2131
July 17, 2006

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100